Original Research

SAGE Open
October-December 2021: 1–12

DOI: 10.1177/21582440211061556
journals.sagepub.com/home/sgo
SAGE

An Exploration of the Psychological Impact of Hacking Victimization

Alexa Palassis[1,2], Craig P. Speelman[1], and Julie Ann Pooley[1]

Abstract

Cybercrime has rapidly grown in prevalence and potential for harm and disruption for victims. Studies have examined the adverse psychological impact of cybercrime for victims; however, the specific effects for victims of hacking are unexplored. The present study aimed to investigate the psychological impacts of hacking victimization through exploration of the experience of victims of hacking. The study employed an in-depth phenomenological approach to explore the experiences of 11 victims of hacking. Semi-structured interviews were used as a tool for data collection, and thematic analysis of the data revealed four main themes: emotional impact; an increased sense of vulnerability; a sense of violation; and coping strategies. The findings highlight that hacking may have significant consequences for victims, and further, that hacking may represent an intrusion into a victim's "digital space." Recommendations are discussed for providing support to victims through measures aimed at increasing victim's self-efficacy, sense of control over their digital environment, and increasing community awareness about the potential adverse impacts for victims of hacking.

Keywords

cyber security, cybercrime, hacking, qualitative, victimization

Introduction

In 2018, 978 million people globally fell victim to online crime, or cybercrime (Symantec Corporation, 2019). Cybercrime refers to a broad range of criminal activity committed using computers or the internet and encompasses a wide range of offenses such as cyber-stalking, harassment, online fraud, phishing and hacking (Morgan et al., 2016). With the rapid digitization of society, trends indicate that cybercrime is a growing issue of economic and social concern, and incidences now considerably exceed rates of traditional crime. To illustrate, 30% of Australian adults fell victim to cybercrime in 2018 (Symantec Corporation, 2019). In contrast, less than 5% of Australian adults were victims of personal crime, and 11% were the victim of household crime (Australian Bureau of Statistics, 2019). Cybercrime results in economic and social damage to governments, private organizations, and individuals, with significant consequences for a growing number of victims in Australia and the world over (Broadhurst, 2017). Cybercrime is considered such a significant issue that the Australian government has recently supported several initiatives to improve organizational and industrial responses to cybercrime (e.g., Cyber Co-operative Research Centre—https://cybersecuritycrc.org.au) and to inform the general populace of the impacts of cybercrime and how to defend against cyber attacks (e.g., Australian Cyber Security Centre—https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-your-family). The focus of the present study is on cybercrime victimization, specifically at the level of individuals.

Typically, cybercrime is conceptualized as a financially motivated or non-violent crime (Smith, 2015). As such, a common perception exists that like other non-violent crime, cybercrime is a "victimless" crime (Kshetri, 2006; Nurse, 2018). This view may stem from the perception that banks tend to compensate victims of financial crimes and therefore no direct cost or harm to the individual exists (Duffield & Grabosky, 2001). Further, the offenses occur in a virtual space, and therefore victims of cybercrime are not real victims as there is no "real" harm involved (Martellozzo & Jane, 2017). However, in recent years, studies have demonstrated that alongside the possible economic damages, cybercrime victims may experience deleterious effects on their emotional and psychological wellbeing, including symptoms similar to those experienced in post-traumatic stress disorder (PTSD) (Cross, 2018; Kirwan & Power, 2011; Symantec

[1]Edith Cowan University, Joondalup, WA, Australia
[2]Cyber Security Cooperative Research Centre, Joondalup, WA, Australia

Corresponding Author:
Craig P. Speelman, School of Arts & Humanities, Edith Cowan University, 270 Joondalup Drive, Joondalup, WA 6027, Australia.
Email: c.speelman@ecu.edu.au

Corporation, 2010). Considering the number of victims facing cybercrime, gaining greater insight into the impacts of victimization is integral to understanding and improving the wellbeing of victims (Green & Pomeroy, 2007a).

Among victims of cybercrime, the most frequently reported victims are those who have experienced hacking. In 2018, a Norton global cybercrime report indicated that the most common cybercrimes involve unauthorized access to home and personal devices and Wi-Fi networks (26%), online banking or other financial accounts (14%), and email accounts (12%) (Symantec Corporation, 2019). In the context of cybercrime, hacking refers to the unauthorized access of data in a computer system or private network, with the intent to exploit information within the system (Morgan et al., 2016). The consequences for the victims may include the redirection of money, malicious damage, and modification or theft of sensitive personal and business data (Nurse, 2018). Despite the magnitude of instances and consequences involved for victims, relatively little is known about the psychological and emotional impact of hacking victimization.

As research into the psychological impacts for cybercrime victims is relatively limited (Jansen & Leukfeldt, 2018; although see a recent UK study by Button et al., 2020), the purpose of the present study was to explore the psychological impact of hacking victimization, as reflected through the experiences of victims of hacking.

Nature and Impact of Crime Victimization

Victimization is a complex process that produces disruptions to daily life. Victims have reported significant variation in the experience and effects of crime, ranging from short-term discomfort to significant long-term effects (DeValve, 2005; Green & Pomeroy, 2007a). The variability of these effects may be related to factors including previous victimization, pre-crime psychological functioning, and in the case of sexual crime, the relationship between the victim and offender (Green & Pomeroy, 2007b; Ruback & Thompson, 2001; Sales et al., 1984). Furthermore, there is evidence to suggest that victimization may be a harmless experience for victims (Hindelang et al., 1978). Researchers have highlighted the difficulty of predicting the type and intensity of effects that individuals will experience following victimization (Christie, 1986; Shapland & Hall, 2007).

Reactions to victimization. A vast amount of research has demonstrated the emotional and psychological impacts of being criminally victimized (Burgess, 1975; Lurigio, 1987). Such effects include indicators of distress such as anxiety, somatization, anger, and low mood (Dignan, 2004; Ruback & Thompson, 2001). The experience of crime also appears to heighten victims' perceived risk and fear of crime, which engenders a loss of trust in others and society (Kury & Ferdinand, 1998; Lurigio, 1987). The adverse effects of victimization have been widely studied using victim survey studies, clinical techniques and in-depth interviews, and the findings generally report that the intensity and severity of the symptoms are specific to the type of offense (Freeman & Smith, 2014; Green & Pomeroy, 2007a; Ruback & Thompson, 2001). For example, violent and sexual crime has been linked to higher levels of distress for victims when compared to victims of property crime (Norris & Kaniasty, 1994). Conversely, studies have suggested that victims of financial crime experience comparative levels of distress to victims of violent crime (Button et al., 2014; Deem et al., 2007). Moreover, Shapland and Hall (2007) found that the proportion of victims who were reported being affected emotionally by crime was similar among victims of violent crime, burglary, and theft. Such research emphasizes the difficulty of predicting the effects of crime victimization and highlights the importance of investigating the effects for specific categories of cybercrime.

Factors Influencing Victim Outcomes

The experience of crime victimization has adverse effects on the beliefs, emotions, and behavior of victims; however, the impact of crime is not the same for all victims. Research in this area indicates that several factors, including appraisal, coping strategies, and social support, are central to enabling positive adaptation after a crime, and determining the likelihood of sustaining long-term psychological harm (Green & Pomeroy, 2007a, 2007b; Ruback & Thompson, 2001). Developing a greater understanding of these factors is integral to improving psychological outcomes for victims of crime.

Rationale

Previous research provides some understanding of the psychological impact of hacking victimization. The findings indicate important factors such as the type and severity of the crime, the victim's appraisal of their experience, coping methods employed and the perception, access and mobilization of social support. However, a limitation exists in the literature. The research has provided insight into the impact of cybercrime for victims of online and banking fraud, stalking and revenge pornography; however, no studies have examined the specific psychological impact for victims of hacking. While quantitative methods enable the collection of large data sets from many participants, there are limitations in the capability to provide detail beyond a list of symptoms. Qualitative methodologies place primary focus and value on understanding in full, the way in which individuals make sense of their experiences within milieus that are interactional, dynamic, and complex in their foundation and structure (Liamputtong, 2009). As such, qualitative methods have often been preferred for investigating experiences of victims of crime, and this has been well demonstrated in cybercrime literature, with in-depth interviews

Table 1. Participant Demographic Characteristics.

	Mr A	Mr B	Mr C	Mr D	Mrs E	Mr F	Ms G	Ms H	Mrs I	Mr J	Mr K
Age	57	58	72	45	56	44	23	33	49	26	47
Gender	M	M	M	M	F	M	F	F	F	M	M
Time Since Crime (±1 year)	−1 year	+1 year	+1 year	−1 year	−1 year	+1 years	+1 year	+1 years	−1 year	−1 year	+1 year
Nature of hacking	Business computers, financial. Personal computer.	Business emails, financial	Business software and website	Home computer, personal information	Mobile phone and bank account	Business website, financial	Phone, personal and professional emails, social media	Personal emails, personal information	Mobile phone and bank account	Personal computer	Business and personal emails, home Wi-Fi cameras

used to explore the perceived impact of victimization. Therefore, the rationale for adopting a qualitative approach for the present study has two components: (a) qualitative methods enable the exploration of novel phenomena that are potentially complex or not well defined, and (b) in-depth methods elicit rich detail from the participant's own viewpoint, in their own words (Liamputtong, 2013).

As the sophistication of technology increases, the number of individuals who will fall victim to cybercrime is set to rise. Considering the prevalence of hacking victims among this group, and the potential consequences for victims, research that aims to enhance understanding of the experiences and effects of victimization is integral to providing support for victims and mitigating the negative effects for victims. Thus, the purpose of the current study was to explore the psychological impacts of cybercrime victimization through an in-depth exploration of the experience of victims of hacking. The research question used to explore this phenomenon was: "What is the lived experience of victimization for victims of hacking?", further underpinned by the question: "What are the perceived psychological effects for victims?"

Method

The methodology employed for the current study was interpretative phenomenology (IP) (Liamputtong, 2013). IP principles aim to represent an interpretative account of how individuals make sense of their experiences, recognizing that researcher and participant are in partnership in the interpretation of meaning (Pietkiewicz & Smith, 2014). To understand the experience of the participant from their perspective and seeking to eliminate biases or attitudes stemming from the researchers, in relation to the phenomena under study, we sought to use an Interpretive Phenomenology approach (Moustakas, 1994).

Participants

Purposive sampling was used to ensure participants who volunteered to be interviewed had been victims of hacking. Inclusion criteria for the study required that participants were (a) self-identified victims of hacking, and (b) 18 years or older. The use of self-identification resulted in a broad range of cases of hacking; from those that had personal and business data accessed and distributed to their social networks, to those who had bank accounts hacked. Inclusion criteria did not exclude participants based on the outcome of the hacking, as the experience of the specific type of cybercrime was of interest rather than the direct effects incurred.

Participants (three females, eight males) ranged in age from 23 to 72 years, with a mean age of 46.36 years. All participants reported being hacked between one to three times via personal devices and accounts and/or business-related devices and accounts. Participant demographic and crime characteristics are reported in Table 1.

Procedure

Upon receiving ethics approval from the Edith Cowan University (ECU) Human Research Ethics Committee (2019-00220-PALASSIS) recruitment commenced through three modes. First, information about the study was presented at a public cyber-security event that was organized by WA AustCyber Innovation Hub, a cyber-security network working with ECU. Members of the audience who were interested in participating in the study were invited to request further information. Second, recruitment flyers were posted around the Joondalup campus of ECU. Third, an article inviting participation was published in a local newspaper. All recruitment efforts occurred in the metropolitan area of Perth, Western Australia. As a result, all participants lived in this area. Prospective participants were emailed study information to inform consent for participation. Interviews were arranged and conducted with an introductory preamble framing the research objective. At each interview, participants signed a consent form before commencing.

A semi structured interview schedule was used to explore the participants' experiences of hacking victimization, their perceptions of the psychological impacts, and the factors relevant to recovery in this context. Semi structured interviews allow the participant to provide information that is most relevant to their experience. In unexplored areas/contexts participants can provide information that is novel, or not considered, within a structured set of questions. Prompts and probes, such as "Can you tell me more about that?" were used to promote expansion into areas of interest identified in the literature, or where the participants diverged from the topic (Pietkiewicz & Smith, 2014).

In line with the dynamic nature of IP, the schedule guided the natural flow of dialog, however the interviewer adapted content of the questions in response to the participant's answers (Breakwell, 2006).

The first author conducted all interviews over a seven-week period; 10 were conducted face-to-face in libraries or cafes, and one was conducted over the phone. An audio recording device was used to record interviews for transcription after each interview. The interviews ran between 25 and 115 minutes, with an average duration of 49 minutes. Data saturation was reached at the 11th interview, evidenced by the information collected providing confirmation of the themes identified, but ceasing to provide new meaning to the data (Morse, 1995). In effect, saturation was reached after the 10th interview. As a further participant had requested to be involved, the opportunity was taken to include the participant to hear if any new information was relayed. Notwithstanding the controversy surrounding data saturation, this current study utilized data or thematic saturation (Sebele-Mpofu & Serpa, 2020). In addition, other aspects of rigor are described below.

Data Analysis

Analysis was conducted based on Braun and Clarke's (2006) thematic analysis procedure and guided by principles of interpretative phenomenological analysis (IPA). The analysis was iterative, and the themes were identified inductively through immersion in the participant's data (Braun & Clarke, 2006).

Initial analysis involved transcription of the interview recordings verbatim, with the omission of names and identifying details; and reading the transcripts, journal entries, and field notes several times (Braun & Clarke, 2006). After establishing familiarity with the data, the first author generated initial codes; made up of words or phrases summarizing sections of the data. Coding involved chunking the data into broader concepts by identifying significant ideas, patterns, and contradictions across the transcripts (Braun & Clarke, 2006). This process was repeated several times for each transcript. From here, codes were analyzed and linked by similarity into potential themes. This stage entailed thinking about connections between the codes and themes, and sorting them into potential themes and subthemes. Thematic maps, like mind maps, were employed to assist this process (Braun & Clarke, 2013). Analysis was cyclic, as earlier transcripts were revisited as new themes were identified from data, and this recursive process strengthened the credibility and confirmability of the interpretations (Braun & Clarke, 2013). All authors were involved with interpreting and further developing the themes, before reviewing, defining and naming the final themes. This process of peer-reviewing provided a form of analytic triangulation and strengthened the credibility of the findings (Creswell & Miller, 2000). Finally, rigor was achieved via several strategies. (1) Scientific rigor was assessed using Braun and Clarke's (2006) 15-point checklist of criteria for good thematic analysis which covered transcription, coding and analysis, recursive reviewing of the transcripts, field notes and journal reflections (Liamputtong, 2009). (2) Use of a transparent audit trail throughout the data collection and analysis process enhanced the dependability of the findings (de Witt & Ploeg, 2006). (3) Member checking increased the credibility of the findings (Creswell & Miller, 2000).

Findings and Interpretations

Employing thematic analysis, we interpreted the participants' accounts into four overarching themes. The themes and 10 associated subthemes summarized in Table 2 encompass the multiple factors that relate to the psychological outcome of hacking victimization. The themes are discussed and related to the current literature and theory to illuminate our findings.

Emotional Impact

The theme of Emotional Impact relates to the affective consequences resulting from the experience of being hacked. Reflecting past victimization research, the participants reported a broad spectrum of experiences or impacts, from minor or no effect to severe, lasting emotional effects (DeValve, 2005; Norris & Kaniasty, 1994). Three subthemes capture the emotional impact for participants: anxiety, depressive symptoms, and secondary victimization.

Anxiety. Consistent with the experience of crime victimization, the participants reported experiencing various states and severity of anxiety linked to being hacked (Dignan, 2004). Some participants reported anxiety in the form of an acute physiological reaction upon realizing they had been hacked, using phrases such as, "my stomach dropped" (Ms G) and "I started panicking" (Mr J). For others, anxiety appeared to manifest in the form of persistent "anguish" and paranoia linked directly to the hacking ordeal. The emotional impact of hacking may be short lived, as some participants reported that their distress and anxiety returned to normal a few weeks after being hacked. For others however, the impact was enduring, with some participants continuing to experience anxiety while using e-commerce, emails or social media sites. In this, Mr J stated "I'm still a little bit paranoid about dealing with everything online." For one participant (Mr K), reminders of the hack in his daily life brought on strong physical reactions: "It only takes one little thing, like if I'm in a servo (fuel station) or something and my bank card gets declined and I literally race out like thunder". In this, Mr K described his experience as a "digital trauma," the stress and anxiety of which was so great that he reported having "a breakdown where I literally collapsed on the floor." When anxiety is linked to a perceived traumatic event, it may be

Table 2. Themes and Subthemes Related to Participants' Experience of Hacking Victimization.

Theme	Subtheme
Emotional impact	Anxiety
	Depressive symptoms
	Secondary victimization
Increased sense of vulnerability	Fear and perceived risk
	Sense of helplessness
	Loss of trust
Sense of violation	Invasion of security and privacy
	Loss of autonomy and control
Coping strategies	Problem-focused coping
	Emotion-focused coping

associated with intrusive recollections such as distressing dreams (Andrews et al., 2003; Bates, 2017):

> I mean I've had like hacking dreams. Like where, where I'm constantly being hacked or where, like, people are hacking nuclear power plants and there's a disaster and like. . . that kind of stuff, like the angst definitely manifests itself. (Mr D)

Moreover, for some participants, distress was visible as they recounted their experience during the interview; as Mr B noted "I'm getting more paranoid now, you know?." Similarly, as Mr K described how he had experienced his Wi-Fi network and personal computer being hacked, he expressed "I've got this feeling right here, now, it's just nauseous you know, just thinking about it." These anecdotes serve to highlight that exposure to reminders of the hacking event may bring on autonomic and emotional reactivity and arousal reactions for some victims; symptoms which are often reported among crime victims as a response to the stress of crime (Sharp et al., 2003). Taken together, anxiety, distressing dreams, paranoia, and emotional or physical reactivity are commonly reported symptoms of acute stress disorder and PTSD among victims of crime (Dignan, 2004). Previous studies have reported anxiety and PTSD related symptoms in victims of online fraud (Cross et al., 2016), cyberstalking (Worsley et al., 2017) and revenge pornography (Bates, 2017), and the participants' reflections provide anecdotal evidence that hacking causes PTSD-like symptoms in some victims.

Depressive symptoms. In addition to anxiety symptomology, the participants frequently described negative emotional effects stemming from the direct and indirect impacts of being hacked. Depressive symptoms were described indirectly, as one participant (Mr J) expressed "I feel really sad and really angry at the same time" when recalling the personal data he had lost, while others expressly stated that they had experienced depression. Mr B stated, "I've had depression before. . .but this certainly brought it on. . . It took me a long time to, to get over it." Another stated:

> I wouldn't be surprised if I was in depression. . .I sort of downplay it a bit but then after I was thinking. . . I didn't lose millions. I lost my livelihood. I lost my identity. . . other people see me as a victim, I see myself as a failed business. (Mr F)

In the above extract, Mr F echoes feelings of failure linked to loss of his business, and the negative attribution he placed on himself as a result. Feelings of loss were also reported, accompanied by guilt:

> It's hard to put a number, it's too hard, but it's loss of my business, my potential to earn at this stage of life. . .It's a bit of an indictment, you know, the way I have failed. (Mr C)

Previous research has found that these negative self-directed thoughts may lead to the emotional elements of depression in victims of crime (Kunst & Koster, 2017). Similarly, some victims reported lowered self-esteem, which appeared to be a central feature in the development of depressive symptoms. In this, Mr K commented, "It was about how to rebuild yourself as a person. . .and how do you get your self-worth back and self-esteem," while Mr F reflected that his self-esteem was "rocked to the core" by the losses incurred through being hacked. Collectively, through the ordeal of being hacked, victims may incur depressive symptoms including lowered self-esteem, feelings of failure and loss, and low mood associated with the direct and indirect effects of the experience, outcomes which have been demonstrated in previous research on victims of traditional and cyber crime (Cross et al., 2016; Dinisman & Moroz, 2017; Fischer & Wertz, 1979; Green & Pomeroy, 2007a).

Secondary victimization. In addition to anxiety and depressive symptoms, the participants expressed frustration about the indirect impacts that being hacked had on their life. Most of the participants spent hours attempting to recover from the effects of the event, and feelings of anger and annoyance appeared to be exacerbated by these efforts. As Mrs I expressed, "I'm probably more just angry. . .and angry, not just even angry at what they did, but angry at the time it's taken to get it right." For another participant, interaction with her service provider was a central source of frustration, Mrs E stated "I was angry, that was a big thing for me. I was just angry. . .I'm angry at the people who were culpable [a telecommunications company] and they will not accept any responsibility whatsoever."

In addition to frustration and anger, participants were distressed by the indirect impact that being hacked had on their social networks:

> It was embarrassment first because I had all these people like, harassing me about trying to stop it and I was like, I can't control . . . . It's like, I'm dealing with my whole life has just exploded on me. (Ms H)

These comments support previous research on cybercrime, in which victims frequently expressed a belief that it is not

possible to repair a negative online image (Symantec Corporation, 2010). A few participants expressed shame and humiliation about having fallen victim to crime. In this, Mr B commented "Even though, they said they would refund it (the money), it's still, it's that kind of bit of humiliation. You know. How could I have been done on this?." Such negative self-directed attributions may contribute to poorer emotional adjustment following victimization, and lead to perceived or actual isolation for victims (Barnett et al., 1996; Janoff-Bulman, 1985). A sense of isolation was apparent for some participants. Mr K described how the embarrassment of having his personal emails and Wi-Fi cameras hacked led to reduced social functioning, remarking that "It's disturbing socially, and now, I literally lock myself away, and I still haven't seen many, many people." The participants often expressed that others were "dismissive" of their emotional reactions. Such perceptions can be stigmatizing and deter victims from seeking social support and inhibit recovery from the emotional impact of victimization (Green & Pomeroy, 2007b).

Increased Sense of Vulnerability

This theme relates to the victim's altered perceptions about their own vulnerability, the world, and others as a result of their experience (Janoff-Bulman & Frieze, 1983). These perceptions are linked to the "Emotional impact" findings, as they may underlie the effects incurred through being hacked. Three sub-themes encompass the personal and social aspects of vulnerability: fear and perceived risk, helplessness, and loss of trust. One participant aptly captured the essence of the theme, stating:

> It's, things will never be the same. You know, I mean, that's, that's it. It's embarrassing. It's paranoia. It's anxiousness. It's about what ifs?. . .It's not so much about rebuilding uh, on the tech side, it's about rebuilding as a person and going 'This is how I have to live now.'(Mr K)

Fear and perceived risk. In line with previous studies, a heightened sense of fear was salient among most participants (Denkers & Winkel, 1998). Fear manifested in three ways: uncertainty about the direct consequences of the crime, increased perceived risk of being hacked, and fear for the future. Uncertainty about the use of their personal data was particularly distressing for some victims:

> They had all my identity documents and that's really concerning for what people could do when they have your identity documents. And the other concern I have is, so there was also things on there when I transferred money to my daughter's account and my son's account and so they got all their details as well. (Mrs E)

Similarly, the extent of the intrusion resulting from being hacked was a source of stress, with many expressing the sentiment that "It was really scary" (Mr K) that the hacker may have "access to everything" (Mrs E). These comments are consistent with Greenberg et al.'s (1983) model of victim decision making, in which fear and anxiety about what might happen in the future is a central source of stress for crime victims.

Fearful cognitions about future victimization were salient among the participants, and often resulted in behaviors aimed at neutralizing the fear by decreasing their perceived risk (Russo & Roccato, 2010). For instance, Mr K stated that "If I see something slightly wrong [when operating online], I look at it and dig deeper. . .So I double check everything." Conversely, for a few participants the experience did appear to engender fear. For instance, one participant (Mr A) commented that "I just thought bugger it! (Laughs). . .because my own clients have had hacks you know. . .we knew it was there, the risk, and really it was what it was." These victims appeared to perceive that they had a high likelihood of being hacked. In consonance, another participant (Ms H) stated "I've been hacked before. . .I just think you're lucky if you haven't been hacked." These comments are distinct from the majority of participants, in that these participants had previous exposure to cybercrime. This is an important finding as it contrasts with previous studies that demonstrated that exposure to crime, direct or vicarious, increases fear of future victimization (Ferraro, 1995; Virtanen, 2017). One explanation for this finding may be that compared to non-victims, individuals who have experienced crime and engaged in successful coping may possess a greater sense of self-efficacy, and the practical skills for coping with future victimization (Bandura, 1977). While these participants did not express a sense of fear, behavioral coping efforts were evident. For instance, Mr A was recruited at a cyber-security event where he was seeking information after being hacked.

Finally, concerns for the state of cybercrime as a problem for society were salient, with the term "wild west" and a "lawless society" common among the participants' accounts. Abstract fear, which concerns the well-being and safety of society is commonly reported among crime victims (Russo & Roccato, 2010):

> That's what's really got me. . .concerned about the future and, and that, that was really the main story that I wanted to share is that like I feel like I've tasted what the future is going to be like. (Mr D)

Fears were expressed on a continuum from a passing feeling for some participants, to impacting the daily thoughts and behaviors of others.

Feelings of helplessness. Participants described feeling unable to defend themselves or act effectively in the face of cybercrime. The sense of helplessness was expressed toward controlling the practical impact and consequent outcomes of being, as Mrs E commented: "I just felt impotent because

there was nothing I could do about it because they had already captured all my information." Helplessness was often expressed alongside fear, as Mr K commented "I looked into it. . .and what I saw really scared me to the core. But that's the world it is." Similarly, the participants expressed negative views about preventing re-victimization:

> The fact that I felt totally helpless and that there's nothing I could do really hammered home to me that like, your average user doesn't really stand much of a chance towards any attack that's dedicated. (Mr D)

Mr H, who is trained and employed in the information technology field, reflected that being equipped with the expertise, but being unable to defend himself served to incur a sense of powerlessness. This notion was consistent with previous literature, which shows that victimization may negatively impact a victims' self-concept, as individuals who viewed themselves as being in control of their own lives may now perceive themselves as powerless (Janoff-Bulman & Frieze, 1983).

Taken together, the sense of helplessness following victimization may incur and accentuate feelings of anxiety and diminished mental health for victims (Dinisman & Moroz, 2017; Worsley et al., 2017).

Loss of trust. Reflective of an increased sense of vulnerability, the findings in this sub-theme relate to distrust toward others and in the internet incurred through being hacked. Specifically, distrust was directed toward the digital environment, as one participant (Ms H) stated "I already didn't trust the internet. . .But I don't trust it more now," while another remarked:

> I can say if I'm honest, I don't feel like trusting anything [online] again. Like unless I'm a hundred percent sure, unless I go deep in and see it's legitimate or not I can't trust another website again. (Mr J)

This is consistent with previous research that has reported that victims commonly experience a loss of trust as a result of victimization (Virtanen, 2017). The "Loss of trust" findings may reflect the notion that victims experience an increased sense of vulnerability as a result of shattered assumptions about others and society as a source of threat (Bard & Sangrey, 1986; Janoff-Bulman & Frieze, 1983).

Sense of Violation

When reflecting on the experience of being hacked, the participants expressed feelings of distress concerning disruptions to security, autonomy, privacy and control. This theme contains two subthemes: violation of privacy and security; and loss of autonomy and control.

Violation of privacy and security. This sub-theme is based on the hypothesis that a source of emotional distress following victimization is a violation of the victim's digital environment as an extension of the self (Bard & Sangrey, 1986; Belk, 1988, 2013). Some participants expressly described feeling "violated" by their experience, while others reflected this notion by expressing a sense that their privacy and security had been invaded. Some participants appeared to reflect the notion that being hacked represented a physical and symbolic intrusion into a private territory. For example, Mrs I stated "I felt like they had been in the house, not remote from. . . somewhere (else)," and another participant (Mr K) likened the experience to "being robbed." Maguire (1980) suggested that victims of home burglary experience stress as a response to the violation of one's safe territory, intimacy and sense of security. This finding may suggest that victims of hacking may experience similar effects to victims of home burglary as a result of an intrusion into a personal territory. A sense that the hackers had accessed their entire connected network was a source of distress reported by some participants:

> I just felt like they'd been in the house. Like the fact that. . .I didn't know where they'd gotten in through the computer, my daughter's Mac or the phone. Have they got hold of my photos? What have they got? (Mrs I)

The "Violation of privacy and security" findings may support the notion that a person's digital environment, and the content within it, are an extension of the self (Belk, 1988, 2013). While knowledge of the psychological impacts of intrusion into private "digital territory" is unexplored, the findings may suggest an expansion of the concept of the extended-self to include the individual's connected devices and digital environment.

Loss of autonomy and control. Findings in this subtheme relate closely to the violation of a person's technologies as an extension of the self, however the source of violation is derived from an invasion of privacy and reduced sense of agency (Kunst & Koster, 2017). When asked how he felt being hacked had impacted him, one participant (Mr K) used the phrase "mind burglary." Another participant expressed:

> I felt like violated, do you know what I mean? Like, you don't hand over anything to anyone and let them go through it, because it's just, I don't know. It's the weirdest feeling I don't know how to explain it. (Ms G)

In the above extract, Ms G is discussing her personal conversations and emails being accessed and shared through her personal and professional networks. The loss of control over what information is shared and what is held private, was particularly distressing, as it represented an imposition on her autonomy and reduced her sense of agency (Figley, 1985; Janoff-Bulman, 1985). Ms G went on to acknowledge the implications of being hacked on her relationship to the internet and her social world. When asked about operating online

after the event, Ms G observed that she is cautious and avoids "putting the digital footprint on any of the ins and outs of people anymore."

> I don't like the fact that they have got photos of my children. Even though they're adults. I don't like the fact that they've got a photo of the cake that I made, or my tennis team. Yeah, it's personal. I don't really use Facebook. You know I don't post on Facebook. . . I don't post photos and things like that. So in a way it's almost, and I don't do that on purpose, so. . .it's almost (like) having an involuntary Facebook. (Mrs E)

Violation was particularly salient among participants who had experienced their personal or home devices being hacked, and of note, the sense of violation reported was not affected by whether the motive of the hack was theft of money, or personal data.

Coping Strategies

This theme relates to the cognitive, behavioral and emotional efforts the participants employed to alleviate the psychological and practical effects of being hacked. Two subthemes emerged: problem-focused coping and emotion-focused coping. Generally, participants engaged in problem-focused efforts immediately following the hacking event and shifted to emotion-focused efforts after the initial reactions had abated.

Problem-focused coping. Participants described a range of behavioral efforts aimed at solving the direct cause of the hack, including formal help seeking, self-educating and modifications to their digital environment. Victims modified their daily routines including using "more secure methods of communication" (Mr D), installing and updating security software restricting their online activity. For instance, Mr B stated "I am more careful now than ever with anything sensitive going over email," and Mrs E commented "I actually don't have Facebook or Messenger anymore." By adopting these behaviors, the victims appeared to be regaining a sense of control over their environment (Lazarus & Folkman, 1984). Lai et al. (2012) identified technological coping which is aimed at restoring security in the digital environment, and conventional problem-focused coping, directed at the self through behavior changes, findings which were congruent with past research on coping behaviors for victims of crime.

Most victims contacted their banks and service providers in order to retrieve accounts and finances, however this behavior often appeared to increase feelings of anger and helplessness, as the participants' efforts were met with a lack of effective support. For instance, Ms H expressed frustration after seeking assistance from her email provider, stating ". . .there was no fix, and then I got really outraged (laughs). So I was just overall kind of like, annoyed too, are you kidding me?" Similarly, Mr F expressed his frustration when his business website was hacked, "There are no contact details for Google. You can't ring Google and say "Um, I've disappeared off the internet. Do you know why?." Mr F echoes the notion that attempts to seek information were futile, as support for hacking victims is not available. Most expressed that their cases were "not important" enough to seek formal support from police or reporting bodies, as Mr J stated "I feel like they [the police] are not giving it much prominence. They should think about the little person as well."

Emotion-focused coping. Participants described strategies aimed at dealing with the emotional effects of being hacked; primarily self-blame, cognitive reappraisal of the event, and seeking support. Many of the participants expressed a sense that they were responsible for their victimization:

> The other thing that gnaws on me is that it was preventable. If I had have updated my software, if I had have looked at my analytics more regularly. They were things that I could have done that could have made it preventable. (Mr F)

Self-blame is commonly reported among crime victims, and may be an adaptive coping strategy, as it increases the victims' reduced sense of control incurred through victimization (Frieze et al., 1987). For instance, in expressing "I don't feel like a victim, because I feel like it is partly my fault" Ms G appears to reflect a notion that she has control over her victim status. Certainly a great deal of the cybercrime literature emphasizes the roles of the victims in their own victimization (Jansen & Leukfeldt, 2016; van de Weijer & Leukfeldt, 2017), but also recognizes that such emphasis can hinder their emotional coping (Jansen & Leukfeldt, 2018). Self-blame may be maladaptive if victimization is attributed to characterological (personality) traits such as being "dumb" or "too trusting" rather than behaviors such as forgetting to lock the front door (Janoff-Bulman, 1985). For example, when discussing the emotional impact of the hacking event, Mr C was visibly tearful as he voiced a sense of personal responsibility stating "I've let my family down." Characterological self-blame has been reported to be associated with decreased feelings of control over future victimization, and poorer psychological adjustment for crime victims (Draucker et al., 2000).

Finally, seeking support was helpful for most participants, and predominately included discussing the event with family and friends. For many participants, this coping strategy was helpful as they could "just express" the emotions incurred. For instance, Mr C commented that "talking gives me therapy." Further, the participants emphasized that sharing their experience provided the opportunity to hear about other hacking victims, and knowing that they were "part of a group of victims" (Mr D) relieved some of the emotional effects. However, in some cases, talking to others appeared to

engender a sense of isolation. For example, Mr K stated that he rarely opens up to others about the emotional impact, because "I just sound like a psycho. . .until someone else gets hacked"; while Mr B expressed that "I don't think my wife could understand why I was so upset about it." However, others found success in seeking support; Mr F noted that social support was integral to "validating" him and aiding his emotional and financial recovery. For this participant, a hack to his website resulted in the demise of his business. Mr B expressed that "in the end I think it's all come down to the support from others." Looking back on their experience, while many participants were not inclined to seek support, many expressed that they did not think emotional support in the sense of "people who could understand what you'd suffered" (Mr B) was available for hacking victims. Findings in the sub-theme of "Emotion-focused coping" are consistent with previous studies that have demonstrated the dual nature of social support in aiding or impeding the recovery process for victims of crime (Andrews et al., 2003; Green & Pomeroy, 2007b).

Closing Summary

The purpose of the present study was to explore the experience of victims of hacking, and provide insight into the psychological impacts of hacking victimization. Adopting an interpretive approach, we collected data through in-depth interviews with 11 self-identified hacking victims. Four main themes were identified that encompass the emotional, cognitive, and behavioral factors relating to the experience of hacking victimization. The experience, and subsequent effects of being hacked, were found to have adverse psychological effects for the participants in this study, consistent with the effects found in the victimization literature, while also being unique to the context of hacking (Deem et al., 2007; Lurigio, 1987; Worsley et al., 2017). In the first theme, the participants described a range of emotional responses including anxiety, depressive symptoms and secondary responses relating to the indirect effects of being hacked. This theme captured the spectrum of the participants' experiences, and the severity and longevity of the reported effects varied among participants. The second theme reveals the participants' altered perception of vulnerability resulting from being victimized. Participants reported a sense of fear as a direct effect of being hacked, future victimization, and abstract fear about the state of cybercrime. Similarly, the participants described a sense of helplessness to defend against future victimization. Participants also expressed a loss of trust for their online environment, and in some cases the loss of trust extended to other people. The third theme relates to a sense of violation of the participant's self, and includes a violation of each participant's security, privacy, autonomy and control. Together the second and third themes revealed changes in beliefs about the self and society. A fourth theme explored the cognitive and behavioral efforts described by participants, with problem focused coping referring to strategies aimed at dealing with the direct impact and source of threat, and emotion-focused coping detailing the strategies aimed at alleviating the stress incurred through being victimized.

Two potential limitations are noted with the current study. Firstly, the participants in this study reported a range of outcomes, in terms of losses and associated psychological impacts, and we have discussed two prominent theories of victimization that may explain these psychological findings. However, qualitative methodologies are unable to confirm the cognitive and psychological impacts reported in this study beyond the sample studied. Further research could assist in exploring broader yet unidentified impacts and/or confirming the current and/or extended impacts through qualitative and quantitative studies in other contexts. Secondly, the use of self-identification meant that the sample included the experiences of victims of business and personal hacking. While common themes were identified, the transferability of the findings to all hacking victims may be limited (Liamputtong, 2009; Smith & Osborn, 2003).

Suggestions for future studies may include investigating the psychological impact of hacking victimization using quantitative measures. As this study adopted an exploratory qualitative methodology, the findings have provided the opportunity for future research to focus attention on specific factors that were identified relating to the psychological impact of hacking. Future research could seek to explore in more depth specific impacts of personal and/or business hacking. In addition, the current study proposed anecdotal support for the theory of the extended self to include a person's technologies and digital environment, and future research may focus on exploring this concept empirically. Finally, considering that coping strategies are consistently linked to victim outcomes, future research may examine the mediating effects of coping strategies for victims of hacking.

Implications

The findings from this study have important implications for clinicians and support organizations working with victims of hacking. The present study adds to the limited existing research on hacking victimization by providing a detailed understanding of the factors related to negative psychological impacts of hacking. These findings have provided a foundation for treatment guidelines for victims of "digital trauma," a phrase coined by one participant. Additionally, the insights gained will enhance understanding for mental health care by enhancing awareness and increasing sensitivity to the needs and issues associated with hacking victimization. Specifically, treatment interventions may include those that promote individual self-efficacy, developing cognitive restructuring skills, and enhancing

support seeking. Furthermore, from a community perspective, reducing stigma through promoting awareness may improve victims' help seeking behaviors. While many of the participants had not previously sought emotional support for their experience, many expressed the positive, cathartic effects of the interview process in providing the opportunity to normalize, and gain reflective insight into their experience. This suggests a need for promoting general awareness of the potential psychological impacts of hacking, and providing support opportunities for cybercrime victims in formats such as support groups. Currently, psychological support for victims of cybercrime is limited within Australia, however private organizations in Europe (Victim Support Europe) and the United Kingdom (Victim Support UK) are seeing success in promoting awareness of the effects of cybercrime victimization, and providing support for people experiencing the effects of cybercrime victimization.

In conclusion, this study is the first to apply an interpretative phenomenological approach to explore the perceived psychological impacts of hacking victimization. The findings in this study suggest that hacking victims may experience many of the same psychological impacts as those experienced in traditional crime. Similar to traditional crime, hacking has negative effects on the emotions, behaviors and beliefs of victims. In hacking however, the salient effects appear to be relevant to issues of online security and privacy, rather than personal safety. At a time when we are experiencing the rapid digitization of society, these findings highlight that this phenomenon should be of concern to the community and mental health professionals.

Acknowledgments

The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

Ethics Statement

Approval for this project was provided by the Edith Cowan University Human Research Ethics Committee (Psychology subcommittee) (2019-00220-PALASSIS).

ORCID iD

Craig P. Speelman https://orcid.org/0000-0001-8629-174X

References

Andrews, B., Brewin, C. R., & Rose, S. (2003). Gender, social support, and PTSD in victims of violent crime. *Journal of Traumatic Stress*, *16*(4), 421–427. https://doi.org/10.1023/A:1024478305142

Australian Bureau of Statistics. (2019). *2017-2018 National Crime Victimisation Survey (Cat. No. 4530.0)*. https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/4530.0Main+Features332017-18?OpenDocument

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295x.84.2.191

Bard, M., & Sangrey, D. (1986). *The crime victim's book* (2nd ed.). Brunner/Mazel.

Barnett, O. W., Martinez, T. E., & Keyson, M. (1996). The relationship between violence, social support, and self-blame in battered women. *Journal of Interpersonal Violence*, *11*(2), 221–233. https://doi.org/10.1177/088626096011002006

Bates, S. (2017). Revenge porn and mental health: A qualitative analysis of the mental health effects of revenge porn on female survivors. *Feminist Criminology*, *12*(1), 22–42. https://doi.org/10.1177/1557085116654565

Belk, R. W. (1988). Possessions and the extended self. *Journal of Consumer Research*, *15*(2), 139. https://doi.org/10.1086/209154

Belk, R. W. (2013). Extended self in a digital world. *Journal of Consumer Research*, *40*(3), 477–500. https://doi.org/10.1086/671052

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2013). *Successful qualitative research: A practical guide for beginners*. Sage.

Breakwell, G. M. (2006). Interviewing. In G. M. Breakwell, S. Hammond, C. Fife-Shaw, & J. A. Smith (Eds.), *Research methods in psychology* (3rd ed., pp. 230–242). SAGE.

Broadhurst, R. (2017). Cybercrime in Australia. In A Deckert & R Sarre (Eds.), *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice* (pp. 221–235). Palgrave Macmillan.

Burgess, A. N. (1975). Family reaction to homicide. *American Journal of Orthopsychiatry*, *45*(3), 391–398. https://doi.org/10.1111/j.1939-0025.1975.tb02550.x

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

Button, M., Sugiura, L., Blackbourn, D., Kapend, R., Shepherd, D., & Wang, V. (2020). *Victims of computer misuse: Main findings*. Report. Retrieved December 2, 2020, from https://researchportal.port.ac.uk/portal/files/20818559/Victims_of_Computer_Misuse_Main_Findings.pdf.

Christie, N. (1986). The ideal victim. In E. A. Fattah (Ed.), *From crime policy to victim policy* (pp. 17–30). Palgrave Macmillan.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory Into Practice*, *39*(3), 124–130. https://doi.org/10.1207/s15430421tip3903_2

Cross, C. (2018). (Mis)Understanding the impact of online fraud: Implications for victim assistance schemes. *Victims & Offenders*, *13*(6), 757–776. https://doi.org/10.1080/15564886.2018.1474154

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, *518*, 1–14. https://apo.org.au/sites/default/files/resource-files/2016-08/apo-nid66438.pdf

Deem, D., Nerenberg, L., & Titus, R. (2007). Victims of financial crime. In R. C. Davis, A. J. Lurigio, & S. Herman (Eds.), *Victims of crime* (3rd ed., pp. 125–145). SAGE.

Denkers, A. J. M., & Winkel, F. W. (1998). Crime victims' well-being and fear in a prospective and longitudinal study. *International Review of Victimology*, *5*(2), 141–162. https://doi.org/10.1177/026975809800500202

DeValve, E. Q. (2005). A qualitative exploration of the effects of crime victimisation for victims of personal crime. *Applied Psychology in Criminal Justice*, *1*(2), 71–89.

de Witt, L., & Ploeg, J. (2006). Critical appraisal of rigour in interpretive phenomenological nursing research. *Journal of Advanced Nursing*, *55*(2), 215–229. https://doi.org/10.1111/j.1365-2648.2006.03898.x

Dignan, J. (2004). *Understanding victims and restorative justice*. McGraw-Hill Education.

Dinisman, T., & Moroz, A. (2017). *Understanding victims of crime: The impact of crime and support needs*. https://www.researchgate.net/profile/Tamar-Dinisman/publication/316787563_Understanding_victims_of_crime_The_impact_of_the_crime_and_support_needs/links/59118a70458515bbcb917314/Understanding-victims-of-crime-The-impact-of-the-crime-and-support-needs.pdf

Draucker, C. B., Stern, P. N., Burgess, A. W., & Campbell, J. C. (2000). Women's responses to sexual violence by male intimates. *Western Journal of Nursing Research*, *22*(4), 385–406. https://doi.org/10.1177/019394590002200403

Duffield, G., & Grabosky, P. (2001). The psychology of fraud. *Trends & Issues in Crime and Criminal Justice*, *199*, 1–6.

Ferraro, K. F. (1995). *Fear of crime: Interpreting victimisation risk* (pp. 24–28). State University of New York Press.

Figley, C. (1985). *Trauma and its wake* (pp. 21–24). Brunner/Mazel.

Fischer, C. T., & Wertz, F. J. (1979). Empirical phenomenological analyses of being criminally victimized. *Duquesne Studies in Phenomenological Psychology*, *3*, 135–158. https://doi.org/10.5840/dspp1979314

Freeman, K., & Smith, N. (2014). Understanding the relationship between crime victimisation and mental health: A longitudinal analysis of population data. *BOCSAR NSW Crime and Justice Bulletins*, *177*, 1–16.

Frieze, I. H., Hymer, S., & Greenberg, M. S. (1987). Describing the crime victim: Psychological reactions to victimization. *Professional Psychology Research and Practice*, *18*(4), 299–315. https://doi.org/10.1037/0735-7028.18.4.299

Greenberg, M., Ruback, R., & Westcott, D. (1983). Seeking help from the police: The victim's perspective. In A. Nadler, J. Fisher, & B. DePaulo (Eds.), *New directions in help: Vol. 3. Applied perspectives on help-seeking and–receiving* (pp. 71–103). Academic Press.

Green, D., & Pomeroy, E. (2007b). Crime victims: What is the role of social support? *Journal of Aggression Maltreatment & Trauma*, *15*(2), 97–113. https://doi.org/10.1300/J146v15n02_06

Green, D. L., & Pomeroy, E. (2007a). Crime victimization: Assessing differences between violent and nonviolent experiences. *Victims & Offenders*, *2*(1), 63–76. https://doi.org/10.1080/15564880600922117

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimisation*. Ballinger.

Janoff-Bulman, R. (1985). The aftermath of victimisation: Rebuilding shattered assumptions. In C. Figley (Ed.), *Trauma and its wake* (Vol. 1, pp. 15–35). Brunner/Mazel.

Janoff-Bulman, R., & Frieze, I. H. (1983). A theoretical perspective for understanding reactions to victimization. *Journal of Social Issues*, *39*(2), 1–17. https://doi.org/10.1111/j.1540-4560.1983.tb00138.x

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. https://doi.org/10.5281/zenodo.58523

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, *6*(2), 205–228.

Kirwan, G., & Power, A. (2011). *The psychology of cyber crime: Concepts and principles*. IGI Global Press.

Kshetri, N. (2006). The simple economics of cybercrimes. *IEEE Security and Privacy*, *4*(1), 33–39. https://doi.org/10.1109/MSP.2006.27

Kunst, M. J., & Koster, N. N. (2017). Psychological distress following crime victimization: An exploratory study from an agency perspective. *Stress and Health*, *33*(4), 405–414. https://doi.org/10.1002/smi.2725

Kury, H., & Ferdinand, T. (1998). The victim's experience and fear of crime. *International Review of Victimology*, *5*(2), 93–140. https://doi.org/10.1177/026975809800500201

Lai, F., Li, D., & Hsieh, C. T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363. https://doi.org/10.1016/j.dss.2011.09.002

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer.

Liamputtong, P. (2009). Qualitative data analysis: Conceptual and practical considerations. *Health Promotion Journal of Australia*, *20*(2), 133–139. https://doi.org/10.1071/HE09133

Liamputtong, P. (2013). *Qualitative research methods* (4th ed.). Oxford University Press.

Lurigio, A. J. (1987). Are all victims alike? The adverse, generalized, and differential impact of crime. *Crime and Delinquency*, *33*(4), 452–467. https://doi.org/10.1177/0011128787033004003

Maguire, M. (1980). The impact of burglary upon victims. *The British Journal of Criminology*, *20*(3), 261–275. https://doi.org/10.1093/oxfordjournals.bjc.a047171

Martellozzo, E., & Jane, E. A. (2017). *Cybercrime and its victims*. Taylor & Francis.

Morgan, A., Dowling, C., Brown, R., Mann, M., Voce, I., & Smith, M. (2016). *Evaluation of the Australian cybercrime online reporting network*. Australian Institute of Criminology.

https://eprints.qut.edu.au/121532/1/acorn_evaluation_report_%281%29.pdf

Morse, J. M. (1995). The significance of saturation. *Qualitative Health Research*, *5*(2), 147–149. https://doi.org/10.1177/104973239500500201

Moustakas, C. (1994). *Phenomenological research methods*. SAGE.

Norris, F. H., & Kaniasty, K. (1994). Psychological distress following criminal victimization in the general population: Cross-sectional, longitudinal, and prospective analyses. *Journal of Consulting and Clinical Psychology*, *62*(1), 111–123. https://doi.org/10.1037//0022-006x.62.1.111

Nurse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), *The Oxford handbook of cyberpsychology* (pp. 663–691). Oxford University Press.

Pietkiewicz, I., & Smith, J. (2014). A practical guide to using interpretative phenomenological analysis in qualitative research psychology. *Czasopismo Psychologiczne: Psychological Journal*, *20*(1), 7–14. https://doi.org/10.14691/cppj.20.1.7

Ruback, R. B., & Thompson, M. P. (2001). *Social and psychological consequences of violent victimisation*. SAGE.

Russo, S., & Roccato, M. (2010). How long does victimization foster fear of crime? A longitudinal study. *Journal of Community Psychology*, *38*(8), 960–974. https://doi.org/10.1002/jcop.20408

Sales, E., Baum, M., & Shore, B. (1984). Victim readjustment following assault. *Journal of Social Issues*, *40*(1), 117–136. https://doi.org/10.1111/j.1540-4560.1984.tb01085.x

Sebele-Mpofu, F. Y., & Serpa, S. (2020). Saturation controversy in qualitative research: Complexities and underlying assumptions. A literature review. *Cogent Social Sciences*, *6*, 1. https://doi.org/10.1080/23311886.2020.1838706

Shapland, J., & Hall, M. (2007). What do we know about the effects of crime on victims? *International Review of Victimology*, *14*(2), 175–217. https://doi.org/10.1177/026975800701400202

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2003). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences*, *49*(1), 131–136. https://doi.org/10.1520/JFS2003178

Smith, J. A., & Osborn, M. (2003). Interpretative phenomenological analysis. In J. A. Smith (Ed.), *Qualitative psychology: A practical guide to research methods* (2nd ed., pp. 53–80). SAGE.

Smith, R. (2015). Trajectories of cybercrime. In R. Smith & R. Cheung (Eds.), *Cybercrime risks and responses: Eastern and western perspectives* (pp. 25–34). Palgrave Macmillan.

Symantec Corporation. (2010). *Cybercrime report: The human impact*. https://community.norton.com/en/blogs/symantec-cyber-education/norton's-cybercrime-report-human-impact-reveals-global-cybercrime

Symantec Corporation. (2019). *Cyber safety insights report global results*. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi05seXwLD0AhW3zjgGHSKCA00QFnoECAYQAQ&url=https%3A%2F%2Fwww.nortonlifelock.com%2Fcontent%2Fdam%2-Fnortonlifelock%2Fpdfs%2Freports%2F2019-nortonlifelock%2520-cyber-safety-insights-report-global-results-en.pdf&usg=AOvVaw0-SOmspnfYB7leZlxqGlVh

van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology Behavior and Social Networking*, *20*(7), 407–412. https://doi.org/10.1089/cyber.2017.0028

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry Psychology and Law*, *24*(3), 323–338. https://doi.org/10.1080/13218719.2017.1315785

Worsley, J. D., Wheatcroft, J. M., Short, E., & Corcoran, R. (2017). Victims' voices: Understanding the emotional impact of cyberstalking and individuals' coping responses. *Sage Open*, *7*(2), 1–13. https://doi.org/10.1177/2158244017710292